



PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2000124952 A

(43) Date of publication of application: 28 . 04 . 00

(51) Int. Cl. H04L 12/56
 G06F 13/00
 H04L 12/46
 H04L 12/28
 H04L 12/26
 H04L 12/66
 H04L 12/54
 H04L 12/58

(21) Application number: 10293245

(22) Date of filing: 15 . 10 . 98

(71) Applicant: NTT DATA CORP

(72) Inventor: BABA TATSUYA
 MATSUDA YOSHIYUKI
 FUCHIZAWA HIROTAKA

(54) METHOD AND SYSTEM FOR TRACKING
 ELECTRONIC DATA AND RECORDING MEDIUM

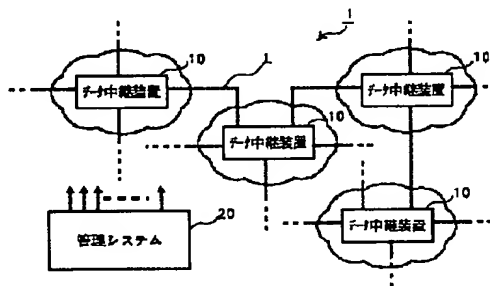
electronic data.

COPYRIGHT: (C)2000,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a data tracking system capable of properly specifying the transmission source of electronic data to be distributed through a network on the side of reception.

SOLUTION: A data tracking system 1 is constituted by providing plural data repeaters 10 chain-connected on the network and a managing system 20 equipped with a means for bidirectionally communicating with the respective data repeaters 10. Each data repeater 10 analyzes the identifier of a low-order layer for carrying electronic data on a network L and based on this analyzed result, the preceding device passing the electronic data is specified. When the specified device is provided with a function equal with the present device, the further preceding another device passing the electronic data is specified. Besides, the analyzed result of the present device is reported to the managing system 20 together with prescribed identification information. Based on the information reported from the respective data repeaters 10, the managing system 20 specifies the distribution route of the relevant



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-124952

(P 2 0 0 0 - 1 2 4 9 5 2 A)

(43) 公開日 平成12年4月28日(2000.4.28)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
H04L 12/56		H04L 11/20	102 D 5B089
G06F 13/00	351	G06F 13/00	351 Z 5K030
H04L 12/46		H04L 11/00	310 C 5K033
12/28		11/12	
12/26		11/20	B

審査請求 未請求 請求項の数18 O L (全11頁) 最終頁に続く

(21) 出願番号 特願平10-293245

(22) 出願日 平成10年10月15日(1998.10.15)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号

(72) 発明者 馬場 達也

東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内

(72) 発明者 松田 栄之

東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内

(74) 代理人 100099324

弁理士 鈴木 正剛

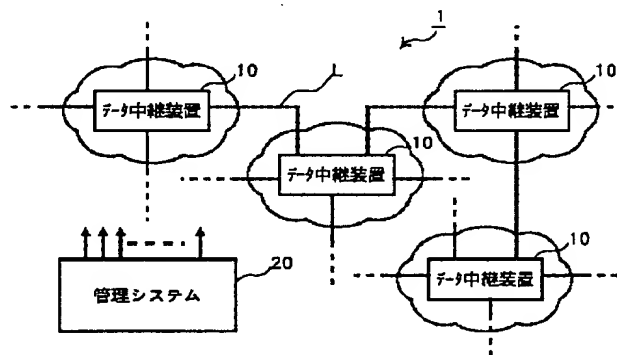
最終頁に続く

(54) 【発明の名称】 電子データの追跡方法及びシステム、記録媒体

(57) 【要約】

【課題】 ネットワークを通じて流通する電子データの発信源を、受信側で正しく特定することができるデータ追跡システムを提供する。

【解決手段】 ネットワーク上で連鎖状に接続された複数のデータ中継装置10と、各データ中継装置10と双方向通信を行う手段を備えた管理システム20とを含んでデータ追跡システム1を構成する。個々のデータ中継装置10は、ネットワークL上で電子データを運ぶ下位層の識別子を解析し、この解析結果に基づいて当該電子データが通過した一つ前の装置を特定し、特定した装置が自装置と同等の機能を備えている装置である場合は、当該電子データがさらに一つ前に通過した他の装置を特定させる。また、自装置での解析結果を所定の識別情報と共に管理システム20に通知する。管理システム20は、各データ中継装置10から通知された情報をもとに当該電子データの流通経路を特定する。



【特許請求の範囲】

【請求項 1】 電子データを流通させる装置が連鎖状に接続されたネットワーク上で前記電子データを運ぶデータリンク層の識別子を解析し、当該電子データが通過した前記装置を前記識別子の解析結果に基づいて特定する過程を含む、電子データの追跡方法。

【請求項 2】 個々の前記装置が前記識別子を解析することで前記電子データが通過した自装置の一つ前の装置を特定した後、この特定した装置に、当該電子データが当該装置の一つ前に通過した他の装置を特定させることを特徴とする、

請求項 1 記載の追跡方法。

【請求項 3】 予め追跡対象となる電子データの特徴情報を特定し、流通する前記電子データが前記特定した特徴情報に合致するときに当該合致する電子データを運ぶデータリンク層の識別子を解析して前記他の装置を特定することを特徴とする、

請求項 1 または 2 記載の追跡方法。

【請求項 4】 それぞれの装置が、前記他の装置を特定できたときは自装置における前記解析の識別情報を当該他の装置及び所定のデータ追跡手段に通知するとともに、前記他の装置を特定できなかったときは当該特徴情報に基づく最終通知情報を前記データ追跡手段に通知することを特徴とする、

請求項 3 記載の追跡方法。

【請求項 5】 流通する電子データの中継を行う複数のデータ中継装置をネットワーク上で連鎖状に接続して成り、

個々のデータ中継装置が、それぞれ、

追跡すべき電子データの特徴情報と追跡結果の通知先アドレスとを含む所定の追跡指示の受信を契機に、自装置を通過する電子データから前記特徴情報に適合するもの（以下、「追跡対象データ」）を探索する第 1 の手段と、

探索した前記追跡対象データを前記ネットワーク上で運ぶデータリンク層の識別子を解析し、この解析結果に基づいて当該追跡対象データが自装置の前に通過した他の装置の特定を試みる第 2 の手段と、

前記他の装置を特定でき且つ特定した装置が自装置と同等の機能を備えている場合に、その装置に対して前記受信した追跡指示と同一内容の追跡指示を与える第 3 の手段と、

自装置における追跡結果を前記通知先アドレス宛に通知する第 4 の手段と、を有することを特徴とする、

電子データの追跡システム。

【請求項 6】 前記第 3 の手段は、前記追跡対象データについて自装置が何番目に追跡指示を受けたかを表す追跡順序情報を前記他の装置宛の追跡指示に添付するように構成され、前記第 4 の手段は、自装置における追跡結果と共に前記追跡順序情報を前記通知先アドレス宛に

通知するように構成されていることを特徴とする、

請求項 4 記載の追跡システム。

【請求項 7】 前記第 3 の手段で他の装置に前記追跡指示を与えることができなかったデータ中継装置が有する前記第 4 の手段は、自装置における追跡結果が前記追跡指示に基づく最終のデータ中継装置である旨を表す付加情報を添付することを特徴とする、

請求項 6 記載の追跡システム。

【請求項 8】 前記第 4 の手段は、前記他の装置のプロトコルアドレスを特定して前記付加情報に添付することを特徴とする、

請求項 7 記載の追跡システム。

【請求項 9】 ネットワーク上で連鎖状に接続された複数のデータ中継装置と、各データ中継装置に対して双方向通信可能に接続されたデータ追跡装置とを含み、

個々のデータ中継装置は、それぞれ、

追跡すべき電子データの特徴情報と前記データ追跡装置のアドレスとを含む所定の追跡指示の受信を契機に、自装置で受信し、他の装置へ転送する電子データから前記特徴情報に適合するもの（以下、「追跡対象データ」）を探索する第 1 の手段と、

探索した前記追跡対象データを前記ネットワーク上で運ぶデータリンク層の識別子を解析し、この解析結果に基づいて当該追跡対象データが自装置の前に通過した他の装置の特定を試みる第 2 の手段と、

前記他の装置を特定でき且つ特定した装置が自装置と同等の機能を備えている場合に、その装置に対して前記受信した追跡指示と同一内容の追跡指示を与える第 3 の手段と、

自装置における追跡結果を前記アドレス宛に通知する第 4 の手段と、を有するものであり、

前記データ追跡装置は、

少なくとも前記第 3 の手段で他の装置に前記追跡指示を与えることができなかったデータ中継装置からの通知情報をもとに当該追跡対象データの発信源を特定するように構成されていることを特徴とする、電子データの追跡システム。

【請求項 10】 ネットワーク上で流通する電子データを受信し、受信した電子データを連鎖状に接続された他の装置へ転送する中継機構と、

追跡すべき電子データの特徴情報と追跡結果の通知先アドレスとを含む所定の追跡指示の受信を契機に、自装置を通過する電子データから前記特徴情報に適合するもの（以下、「追跡対象データ」）を探索する第 1 の手段と、

探索した前記追跡対象データを前記ネットワーク上で運ぶデータリンク層の識別子を解析し、この解析結果に基づいて当該追跡対象データが自装置の前に通過した他の装置の特定を試みる第 2 の手段と、

前記他の装置を特定でき且つ特定した装置が自装置と

10

20

30

40

50

等の機能を備えている場合に、その装置に対して前記受信した追跡指示と同一内容の追跡指示を与える第 3 の手段と、

自装置における追跡結果を所定の識別情報と共に前記通知先アドレス宛に通知する第 4 の手段と、を有することを特徴とする、

データ中継装置。

【請求項 1 1】 前記第 4 の手段は、前記第 3 の手段で他の装置に前記追跡指示を与えることができなかった場合にのみ前記通知を行うことを特徴とする、

請求項 1 0 記載のデータ中継装置。

【請求項 1 2】 ネットワーク上で連鎖状に接続された複数のデータ中継装置及び前記ネットワークを流通する電子データの到達先に備えられた装置との間で通信を行う通信手段と、

追跡すべき電子データの到達先の直前のデータ中継装置を特定し、特定したデータ中継装置宛てに当該到達先より知得した前記追跡すべき電子データの特徴情報及び自装置のアドレスを含む追跡指示を発行する手段と、

前記追跡指示の宛先となるデータ中継装置またはそのデータ中継装置が前記追跡指示と同一の追跡指示を与えた他のデータ中継装置より受領した通知情報に基づいて前記特徴情報に適合した電子データの流通経路を解析する手段とを有することを特徴とする、データ追跡装置。

【請求項 1 3】 前記到達先に備えられた不正アクセスセンサの種別毎に、攻撃パターンとそのときのセンサ出力コードとを対応付けて記録した第 1 記録手段と、

前記センサ出力コードの受領を契機に前記第 1 記録手段を参照して該当する攻撃パターンとその攻撃パターンに対応する前記特徴情報を特定する手段と、

をさらに有する、請求項 1 2 記載のデータ追跡装置。

【請求項 1 4】 前記不正アクセスセンサの種別とそのセンサを採用するシステムの管理者のメールアドレスとを登録しておき、所定の場合に前記管理者のメールアドレス宛てに警告メールを自動送信する手段をさらに有する、

請求項 1 3 記載のデータ追跡装置。

【請求項 1 5】 前記流通経路を解析して攻撃者を特定したときに当該攻撃者または攻撃者に関わる者宛に警告メールを発信する手段をさらに有する、

請求項 1 4 記載のデータ追跡装置。

【請求項 1 6】 ネットワーク上で連鎖状に接続された他の装置及び所定のデータ追跡装置と双方向通信可能に接続されたコンピュータ装置に下記の処理を実行させるためのプログラムコードが記録された、コンピュータ読取可能な記録媒体。

(1) 追跡すべき電子データの特徴情報と追跡結果の通知先アドレスとを含む所定の追跡指示の受信を契機に、自装置で受信し前記他の装置のいずれかへ転送する電子データから前記特徴情報に適合するもの (以下、「追跡

対象データ」) を探索する処理、(2) 探索した前記追跡対象データを前記ネットワーク上で運ぶデータリンク層の識別子を解析し、この解析結果に基づいて当該追跡対象データが自装置の前に通過した他の装置の特定を試みる処理、(3) 前記他の装置を特定でき且つ特定した装置が自装置と同等の機能を備えている場合に、その装置に対して前記受信した追跡指示と同一内容の追跡指示を与える処理、(4) 自装置における追跡結果を所定の識別情報と共に前記通知先アドレス宛に通知する処理。

10 【請求項 1 7】 ネットワーク上で連鎖状に接続された複数のデータ中継装置及び前記ネットワークを流通する電子データの到達先に備えられた装置との間で通信を行う通信手段を備えたコンピュータ装置に下記の処理を実行させるためのプログラムコードが記録された、コンピュータ読取可能な記録媒体。

(1) 前記到達先に備えられた装置より追跡すべき電子データの特徴情報を知得する処理、(2) 前記到達先の直前のデータ中継装置を特定し、特定したデータ中継装置宛てに前記知得した特徴情報及び自装置のアドレスを含む追跡指示を発行する処理、(3) 前記追跡指示の宛先となるデータ中継装置またはそのデータ中継装置が前記追跡指示と同一の追跡指示を与えた他のデータ中継装置より受領した通知情報に基づいて前記特徴情報に適合する電子データの流通経路を解析する処理。

【請求項 1 8】 前記各処理の一部を前記コンピュータ装置に搭載されたオペレーティングシステムに実行させるためのデジタル情報が記録された、請求項 1 6 または 1 7 に記載された記録媒体。

【発明の詳細な説明】

30 【0 0 0 1】

【発明の属する技術分野】本発明は、例えばインターネットを介して流通する電子データの流通経路または発信源を、送信元プロトコルアドレスが偽れた場合であっても正確に特定できるようにするためのデータ追跡技術に関する。

【0 0 0 2】

【従来の技術】インターネット等の通信網を用いて電子データの送受信を行う場合、その電子データには、宛先プロトコルアドレスと送信元プロトコルアドレスが付与される。そのため、電子データを受信したシステムでは、その電子データに付与された送信元プロトコルアドレスを調べることによって、どの装置またはシステムから送られてきたのか、つまり発信源を確認できるようになっている。

【0 0 0 3】

【発明が解決しようとする課題】しかし、送信元プロトコルアドレスは、送信元システムによって任意に付与されるものなので、これを偽ることにより送信元システムを隠すことは容易である。通常、あるシステムに不正にアクセスする者 (以下、不正アクセスを「攻撃」、不正

アクセスを行う者を「攻撃者」と称する場合がある）は、身元を隠すために自己のシステムの送信元プロトコルアドレスではなく、別のシステムのプロトコルアドレスを用いて攻撃する場合が多い。この場合、不正にアクセスされたシステム側では、送信元プロトコルアドレスを信用することができず、また、攻撃者を正しく特定することができないという問題があった。

【0004】そこで本発明は、電子データを受信した側で、その電子データの送信元を正しく特定することができる電子データの追跡方法を提供することを課題とする。本発明の他の課題は、この追跡方法の実施に適した電子データの追跡システム及びその構成装置を提供することにある。

【0005】

【課題を解決するための手段】上記課題を解決する本発明の追跡方法は、電子データを流通させる装置が連鎖状に接続されたネットワーク上で前記電子データを運ぶデータリンク層の識別子を解析し、当該電子データが通過した前記装置を前記識別子の解析結果に基づいて特定する過程を含むことを特徴とする。より具体的には、個々の前記装置が前記識別子を解析することで前記電子データが通過した自装置の一つ前の装置を特定した後、この特定した装置に、当該電子データが当該装置の一つ前に通過した他の装置を特定させる。

【0006】好ましくは、予め追跡すべき電子データの特徴情報を特定しておき、流通する前記電子データが前記特徴情報に合致するときに、当該合致する電子データを運ぶデータリンク層の識別子を解析するようにする。また、それぞれの装置が、前記他の装置を特定できたときは自装置における前記解析の識別情報を当該他の装置及び所定のデータ追跡手段に通知するとともに、前記他の装置を特定できなかったとき（前記識別子を解析することで前記電子データが通過した自装置の一つ前の装置を特定する機能を持つ装置でない場合を含む）は当該特徴情報に基づく最終通知情報を前記データ追跡手段に通知するようにしても良い。

【0007】上記他の課題を解決する本発明の追跡システムは、流通する電子データの中継を行う複数のデータ中継装置をネットワーク上で連鎖状に接続して成る。あるいは、これらのデータ中継装置に対して双方向通信可能に接続されたデータ追跡装置とを含んで成る。個々のデータ中継装置は、それぞれ下記の要素を有するものである。

（1-1）追跡すべき電子データの特徴情報と追跡結果の通知先アドレス（例えば、データ追跡装置のアドレス）とを含む所定の追跡指示の受信を契機に、自装置を通過する電子データから前記特徴情報に適合するもの（追跡対象データ）を探索する第1の手段、（1-2）探索した前記追跡対象データを前記ネットワーク上で運ぶデータリンク層の識別子を解析し、この解析結果に基

づいて当該追跡対象データが自装置の前に通過した他の装置の特定を試みる第2の手段、（1-3）前記他の装置を特定でき且つ特定した装置が自装置と同等の機能を備えている場合に、その装置に対して前記受信した追跡指示と同一内容の追跡指示を与える第3の手段、（1-4）自装置における追跡結果を前記通知先アドレス宛に通知する第4の手段。

【0008】この第4の手段は、好ましくは、自装置における追跡結果と共に、当該追跡結果が何番目の追跡結果かを表す追跡順序情報を前記通知先アドレスに通知するように構成し、前記第3の手段で他の装置に前記追跡指示を与えることができなかった場合は、自装置が前記追跡指示に基づく最終のデータ中継装置である旨の付加情報を添付するように構成する。当該他の装置のプロトコルアドレスが特定できた場合は、そのプロトコルアドレスをも添付するように構成する。前記データ追跡装置を設ける場合は、少なくとも前記第3の手段で他の装置に前記追跡指示を与えることができなかったデータ中継装置からの通知情報をもとに当該追跡対象データの発信源を特定するように、それを構成する。

【0009】本発明はまた、上記データ追跡システムの一部を構成するデータ中継装置、データ追跡装置、及びこれらの装置をコンピュータ装置により実現するための記録媒体を提供する。

【0010】本発明のデータ中継装置は、下記の要素を有するものである。

（2-1）ネットワーク上で流通する電子データを受信し、受信した電子データを連鎖状に接続された他の装置へ転送する中継機構、（2-2）追跡対象データの特徴情報と追跡結果の通知先アドレスとを含む所定の追跡指示の受信を契機に、自装置を通過する電子データから追跡対象データを探索する第1の手段と、前述の第2乃至第4の手段を備えたデータ追跡機構。

【0011】本発明のデータ追跡装置は、下記の要素を有するものである。

（3-1）ネットワーク上で連鎖状に接続された複数のデータ中継装置及び前記ネットワークを流通する電子データの到達先に備えられた装置との間で通信を行う通信手段、（3-2）前記到達先に備えられた装置より知得した、追跡対象となる電子データの特徴情報に基づいて、当該到達先の直前のデータ中継装置を特定し、特定したデータ中継装置宛てに前記特徴情報及び自装置のアドレスを含む追跡指示を発行する手段、（3-3）前記追跡指示の宛先となるデータ中継装置またはそのデータ中継装置が前記追跡指示と同一の追跡指示を与えた他のデータ中継装置より受領した通知情報に基づいて前記追跡対象データの流通経路を解析する手段。

【0012】好ましい実施の形態では、上記（3-1）～（3-3）のほかに、前記到達先に備えられた不正アクセスセンサの種別毎に攻撃パターンとそのときのセン

サ出力コードとを対応付けて記録した第1記録手段と、前記センサ出力コードの受領を契機に前記第1記録手段を参照して該当する攻撃パターンとその攻撃パターンに対応する前記特徴情報を特定する手段とを具備し、必要に応じて、前記不正アクセスセンサの種別とそのセンサを採用するシステムの管理者のメールアドレスとを登録元毎に記録しておき所定の場合に前記管理者のメールアドレス宛てに警告メールを自動送信する手段と、前記流通経路を解析して攻撃者を特定したときに当該攻撃者または攻撃者に関わる者宛に警告メールを発信する手段とをさらに具備してデータ追跡装置を構成する。

【0013】本発明の記録媒体は、データ中継装置を構成するためのもので、ネットワーク上で連鎖状に接続された他の装置及び所定のデータ追跡装置と双方向通信可能に接続されたコンピュータ装置に下記の処理を実行させるためのプログラムコードが記録された、コンピュータ読取可能な記録媒体である。

(4-1) 追跡すべき電子データの特徴情報と追跡結果の通知先アドレスとを含む所定の追跡指示の受信を契機に、自装置で受信し前記他の装置のいずれかへ転送する電子データから追跡対象データを探索する処理、(4-2) 探索した前記追跡対象データを前記ネットワーク上で運ぶデータリンク層の識別子を解析し、この解析結果に基づいて当該追跡対象データが自装置の前に通過した他の装置の特定を試みる処理、(4-3) 前記他の装置を特定でき且つ特定した装置が自装置と同等の機能を備えている場合に、その装置に対して前記受信した追跡指示と同一内容の追跡指示を与える処理、(4-4) 自装置における追跡結果を所定の識別情報と共に前記通知先アドレス宛に通知する処理。

【0014】本発明の他の記録媒体は、データ追跡装置を構成するためのもので、ネットワーク上で連鎖状に接続された複数のデータ中継装置及び前記ネットワークを流通する電子データの到達先に備えられた装置との間で通信を行う通信手段を備えたコンピュータ装置に下記の処理を実行させるためのプログラムコードが記録された、コンピュータ読取可能な記録媒体である。

(5-1) 前記到達先に備えられた装置より追跡すべき電子データの特徴情報を知得する処理、(5-2) 当該到達先の直前のデータ中継装置を特定し、特定したデータ中継装置宛てに前記知得した特徴情報及び自装置のアドレスを含む追跡指示を発行する処理、(5-3) 前記追跡指示の宛先となるデータ中継装置またはそのデータ中継装置が前記追跡指示と同一の追跡指示を与えた他のデータ中継装置より受領した通知情報に基づいて追跡対象データの流通経路を解析する処理。

【0015】なお、上記各記録媒体において、前記各処理の一部を前記コンピュータ装置に搭載されたオペレーティングシステムに実行させるためのデジタル情報を記録するようにしても良い。

【0016】

【発明の実施の形態】次に、本発明の電子データの追跡方法の実施の形態を説明する。本発明では、送信元プロトコルアドレスや送信先プロトコルアドレスよりも下位に位置する層（以下、この下位層を総称したものを「データリンク層」とする）のフレームまたはセル（以下、両者を区別する必要がない場合は「フレーム等」と略称する）に含まれる識別子をもとに、電子データの通過してきた経路を受信側から送信側に向かって逆に辿っていく。ここで、「識別子」とは、電子データを運ぶメディアがLAN (Local Area Network) の場合はMAC (Media Access Control) アドレス、フレームリレー網の場合はDLCI (Data Link Connection Identifier)、ATM (Asynchronous Transfer Mode) 網の場合はVPI (Virtual Path Identifier) / VCI (Virtual Channel Identifier) 等の情報である。

【0017】上記メディアとしては、イーサネット（登録商標）やFDDI (Fiber Distributed Data Interface) 等を用いたLANや、専用線、フレームリレー網、ATM網等が使用される。専用線を介して装置（データを発信した装置／システム／データ中継装置等）が接続される場合には、一つのインタフェースに対して、一つの装置しか接続されないため、辿るべき経路は一意に決定される。フレームリレー網やATM網の場合も、PVC (相手先固定) 接続の場合には、接続される相手装置とDLCI (フレームリレー網の場合)、VPI / VCI (ATM網の場合) が1対1に対応しているため、追跡すべき電子データが含まれるデータリンク層のフレーム等のDLCIやVPI / VCIを確認すれば、一つ前の装置を特定することができる。LANの場合は、そのフレームに送信元MACアドレスが付与されるので、そのMACアドレスから一つ前の装置を特定することができる。

【0018】但し、フレーム等に含まれる識別子は、通常、そのフレーム等が送信されるLANやフレームリレー網、ATM網等を介した際のデータ中継装置のものであるので、隣の装置までは特定できても、発信元の装置までは直ちに特定することができない。そこで、この実施形態では、フレーム等の識別子から、追跡すべき電子データが通過した一つ前の装置をまず特定し、その装置上で、追跡すべき電子データの特徴情報に適合する電子データ（これが追跡対象データとなる）を再び捕捉し、その追跡対象データのフレーム等の識別子を調べることによって、さらに先の装置を探索していくという動作を繰り返していく。このような動作を繰り返していくことで、最終的に追跡対象データの発信源を特定する。

【0019】上述の追跡方法は、例えば、図1に示すように構成されるデータ追跡システムによって実施することができる。このデータ追跡システム1は、既存の通信システムや内部ネットワーク等が接続され、公衆通信

10

20

30

40

50

網、例えばインターネット上で連鎖状に接続された複数のデータ中継装置 10 と、各データ中継装置 10 との間で双方向通信ができる形態で接続されたデータ追跡装置（この実施の形態では、「管理システム」と称する）20 とを含んで構成されるものである。以後、通信システムや内部ネットワークのうち、攻撃者が操作したものを「発信源装置」、攻撃された通信システム等を「被害者ネットワーク」と称する。被害者ネットワークには、攻撃者による不正アクセスの事実を検知するための装置、（以下、「センサ」：図示省略）が備えられており、このセンサで攻撃パターンが検知されたときに、その旨と追跡すべき電子データの特徴情報が、自センサの識別子と共に管理システム 20 に通知されるようになってい

【0020】各データ中継装置 10 は、例えば中継機構を備えた既存の「ルータ」に、データ追跡機構を付加することで実現が可能である。中継機構は、特定の通信機器等から発信された電子データを、他のデータ中継装置 10 を含む最適ルートを通じて宛先となるシステム（以下、「宛先システム」）へ中継する機構である。

【0021】データ追跡機構は、フレーム等の識別子、例えば LAN の場合は MAC アドレス、フレームリレー網の場合は DLCI、ATM 網の場合は VPI/VC I 等の情報をもとに、電子データが通過してきた経路を受信側から送信側に向かって辿っていくためのもので、図 2 に示すように、指示データ受領部 11、データ捕捉部 12、データ比較部 13、装置等特定部 14、通知部 15 の機能を含んで構成される。

【0022】指示データ受領部 11 は、被害者ネットワークが攻撃されたときに、管理システム 20 から追跡指示と共に取得した、追跡対象データの特徴情報、すなわち送信元 IP アドレス、宛先 IP アドレス、その上位プロトコルの種類等の情報と、追跡結果の通知先アドレスである管理システム 20 のアドレスと、追跡 ID とを保持しておくものである。「追跡 ID」は、個々の追跡対象データを識別するための情報である。これは、追跡対象データが複数の場合に有効となる。

【0023】データ捕捉部 12 は、自装置を通過する電子データを捕捉するものであり、データ比較部 13 は、捕捉された電子データの特徴情報と追跡すべき電子データの特徴情報とを比較して一致するものを特定するものである。

【0024】装置等特定部 14 は、追跡対象データが特定されたときにそれを運ぶフレーム等の識別子を調べることにより、一つ前の他のデータ中継装置及びその IP アドレスを特定するものである。具体的には、装置毎の IP アドレスとフレーム等の識別子、例えば MAC アドレスとを対応付けた ARP (Address Resolution Protocol) を有しており、この ARP テーブルを参照することによって、データ中継装置等を特定する。

【0025】通知部 15 は、MAC アドレスを特定したデータ中継装置に、自装置が受領した上述の追跡指示と同一内容の追跡指示を通知するとともに、管理システム 20 に自装置の追跡結果を通知する機能を有するものである。追跡指示及び追跡結果の通知に際しては、自装置における追跡結果が何番目の追跡結果かを表す追跡順序情報を生成し、これを添付する。追跡順序情報は、具体的には、管理システム 20 から最初に追跡指示を受けた最初のデータ中継装置を起算点とするシーケンシャル番号であり、追跡指示を次のデータ中継装置に通知する際に“1”ずつインクリメントする。次のデータ中継装置を特定できなかったときは、自装置がその追跡対象データについての最終のデータ中継装置であることを意味するので、管理システム 20 宛の追跡順序番号に代えて、あるいは追跡順序番号と共に、最終であることを表すフラグ等を添付する。なお、次のデータ中継装置を特定できなかった場合の態様として、装置特定のための処理、あるいは追跡対象データの探索についての処理が一定時間経過しても完了しなかった場合を含めるようにしても良い。つまり、上記各処理がタイムアウトした場合に、エラーと共に、自装置での追跡が最終であることを表すフラグ等を添付するようにする。また、通信対象データが通過した一つ前の装置は特定できたが、それがデータ中継装置でなく、且つその装置の IP アドレスを特定できたときは、この IP アドレスを管理システム 20 に通知するようにする。

【0026】このような機能を有する複数のデータ中継装置 10 を用いて発信源装置を追跡するための原理を模式的に示したのが図 3 である。図 3 (a) は発信源装置 30 からインターネットを通じて発信され、流通する電子データの構造図、同 (b) は、到達先がデータ中継装置 10 c の後の被害者ネットワーク（その中の通信装置またはシステム）である場合に、このデータ中継装置 10 c と他のデータ中継装置 10 a、10 b との協働処理によって発信源装置 30 を特定する場合の手順 (①～⑦) を示した図である。

【0027】追跡すべき電子データは、例えばパケット状のもので、図 3 (a) に示されるように、最初にフレーム等のヘッダ 31、次いで IP ヘッダ 32、その後にデータ成分 33 が配置されるようになっている。この電子データは、図 3 (b) に示されるように、発信源装置 30 から最初にデータ中継装置 10 a を介してインターネットに発信され、次いで、データ中継装置 10 b、データ中継装置 10 c でそれぞれ中継されて被害者ネットワークに到達する。管理システムは、被害者ネットワークに接続されたセンサからの依頼に基づいて、センサの一つ前のデータ中継装置 10 c を特定し、このデータ中継装置 10 c に、追跡すべき電子データの特徴情報や追跡結果の通知先アドレス（自己のアドレス）を含む追跡指示を通知する。

【0028】データ中継装置10cは、この追跡指示の受信を契機に自装置を通過する電子データから追跡対象データに該当するものを捕捉してそのデータリンク層を解析し、送信元のMACアドレスを調べる。これにより、一つ前のデータ中継装置10bが特定されるので、自装置における追跡結果を追跡順序識別情報と共に管理システムへ通知し、さらに、データ中継装置10bへ同一内容の追跡指示を通知する。データ中継装置10bも、データ中継装置10cと同様の手順で追跡対象データが通過した一つ前のデータ中継装置10aを特定する。そして、自装置の追跡結果等を管理システムへ通知するとともにデータ中継装置10aへ自装置による追跡順序識別情報と同一内容の追跡指示とを通知する。

【0029】データ中継装置10aでも同種の追跡処理を行うが、その一つ前には同等の機能を有する装置が存在しないので、目的の発信源装置30、あるいは発信源装置30の所属する組織のネットワークまで辿り着いたことになる。そこで、発信源装置30のIPアドレスを特定し、このIPアドレスを自装置の追跡結果等と共に管理システム20に通知する。このときのIPアドレスは、当該発信源装置30が通常のデータ通信を行ううえで欠かせないMACアドレスからARPテーブル等を利用して得られたものであり、これを発信源装置30側で攻撃者が偽ることは事実上不可能である。このようにして、発信源装置30を正確に特定することができる。

【0030】データ中継装置10による上述のデータ追跡機構の機能は、個々のデータ中継装置本体にCPUとメモリとを設け、メモリに所定のプログラムコードをCPUが読みとれる形態で記録しておくことで実現することができる。また、CPUが上記プログラムコードを実行することによって各機能ブロックが形成されるだけでなく、そのプログラムコードの指示に基づいてオペレーティングシステム(OS)が実際の処理の一部を行い、その処理を通じて上記各機能ブロックが形成されるようにしても良い。エージェントを組み込んでデータ追跡機構の機能を実現するにすれば、データ中継装置10の構成をより簡略化することができる。

【0031】管理システム20は、被害者ネットワークのセンサや各データ中継装置10等からの通知情報をもとに電子データの流通経路を管理するためのもので、所定のOSのもとで動作するコンピュータシステムによって実現される。この管理システム10は、図4に示すように、被害者ネットワークを含む種々のネットワークに設置されたセンサや各データ中継装置10等との間で双方向通信を行うための通信制御機構21、攻撃パターンデータベース22、不正アクセス発信元統計ファイル23、不正アクセス状況統計ファイル24、登録センサ情報ファイル25のほか、コンピュータシステム本体のCPUが所定の記録媒体に記録されたプログラムコードを読み込んでOSと共に協同実行することによって形成さ

れる、追跡指示部26、経路管理部27、警告部28の機能ブロックを少なくとも具備している。

【0032】攻撃パターンデータベース22は、例えば被害者ネットワークのセンサが検知する攻撃パターンと検知時に出力されるコードが、そのセンサの製造メーカによってまちまちである点に鑑み、センサ毎に攻撃パターンとそのときの出力コードとを対応付け、一律的な処理を行えるようにするものである。必要に応じて重大度も対応付けておき、センサからの出力コードが複数の場合に、いずれかを優先的に処理できるようにする。新しいセンサが使用された場合は、そのセンサの識別情報とそのセンサが検出する攻撃パターン、出力コード、重大度が追加記録されるようになっている。図5は、この攻撃パターンデータベース22の内容の一例を示した図表である。

【0033】不正アクセス発信元統計ファイル23は、攻撃者が特定されたときに、そのときの攻撃パターン、日時、回数等を攻撃者毎に蓄積したものであり、不正アクセス状況統計ファイル24は、検知された攻撃パターンの数をパターン毎に蓄積したものである。これらのファイルは、警告メール等を発するときに使用される。図6は不正アクセス発信元統計ファイル23、図7は不正アクセス状況統計ファイル24の内容例を示した図表である。

【0034】登録センサ情報ファイル25は、使用センサの種別、使用センサの識別子(アドレス若しくはベンダ固有の文字列)、管理者の連絡先、使用センサの直上の(つまり追跡始点となる)データ中継装置のアドレスを登録したものである。これによって、どの登録元がどの種類のセンサを使用しているかを知ることができるようになっている。図8は、この登録センサ情報ファイル25の内容例を示した図表である。

【0035】追跡指示部26は、被害者ネットワークのセンサから、検知した攻撃パターンを受領するとともに、その被害者ネットワークのセンサのアドレス等の識別子から、登録センサ情報ファイル25を参照することにより、センサの一つ前のデータ中継装置10のIPアドレスを特定し、特定したデータ中継装置10宛てに、上述の追跡指示を通知するものである。

【0036】経路管理部22は、複数のデータ中継装置10からの追跡結果の通知に基づいて各データ中継装置10を通過した追跡対象データの流通経路を管理し、発信源装置、及び/又は、その管理者を特定するものである。

【0037】警告部23は、以下の場合に警告メールを発信するものである。

(1) センサから攻撃の通知を受けた場合において、その攻撃パターンをサポートしていないセンサがあるかどうかを攻撃パターンデータベース22をもとに調査し、有る場合はそのセンサを使用している登録元を登録セン

10

20

30

40

50

サ情報ファイル 25 から探し出して、その管理者に注意を促すための警告メールを自動的に発信する。

(2) 被害者ネットワークのセンサの管理者に対し、不正アクセス発信元統計ファイル 23 で規定した重大度や、不正アクセス状況統計ファイル 24 に蓄積された検知数が規定値に達したときに警告メールを自動的に発信する。

(3) 攻撃者の管理者宛に警告メールを発信する。攻撃者の管理者のメールアドレスは、発信源装置の IP アドレスから DNS (Domain Name Service) の逆引き機能や WHOIS データベースを利用することにより割り出すことができる。WHOIS データベースは、アドレスやドメイン名をキーにして、利用している IP アドレス、ドメイン (組織) 名、管理者のアドレスをオンライン検索することができる公知のデータベースである。

【0038】なお、上記プログラムコードを記録した記録媒体は、通常、CPU が随時読み取り可能な固定型ディスクや半導体メモリであるが、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、DVD、磁気テープ等の可搬性メディア、あるいはコンピュータがアクセス可能なプログラムコードサーバ等に記録されて流通し、運用時に上記固定型ディスクにインストールされるものであっても良い。また、CPU が上記プログラムコードを実行することによって各機能ブロック 26 ~ 28 が形成されるだけでなく、そのプログラムコードの指示に基づいて OS が実際の処理の一部を行い、その処理を通じて上記各機能ブロック 26 ~ 28 が形成されるようにしても良い。

【0039】次に、上記のように構成されるデータ追跡システム 1 の運用手順を、図 9 の手順図に従って具体的に説明する。ここでは、各データ中継装置 10 を通過する電子データ (及び追跡対象データ) が一定サイズのケットであるものとする。被害者ネットワークのセンサが、攻撃パターンと追跡すべきケットの特徴情報とを管理システム 20 に通知する (ステップ S101)。通知を受けた管理システム 20 は、この特徴情報や追跡結果の通知アドレスを含む追跡指示を被害者ネットワークの一つ前のデータ中継装置 10 に組み込まれたデータ追跡機構に伝える (ステップ S102)。

【0040】追跡指示を受けたデータ中継装置 10 は、自装置において追跡すべき経路が複数あるかどうかを調べ、複数の経路がある場合は、管理システム 20 から渡された特徴情報と一致するケットを監視する (ステップ S103 : Yes、S104)。該当するケットが通過したときは、それを追跡対象ケットとして捕捉し、この追跡対象ケットが通過したインタフェースを特定する (ステップ S105 : Yes、S106)。

【0041】インタフェースがイーサネット、FDDI 等の LAN であった場合は、追跡対象ケットに含まれている送信元の MAC アドレスを調べて一つ前の装置を

特定する (ステップ S108a)。インタフェースがフレームリレー網であった場合は、その追跡対象ケットが含まれているデータリンク層フレームの DLCI から相手側装置を特定する (ステップ S108b)。インタフェースが ATM 網であった場合は、その追跡対象ケットが含まれているセルの VPI/VCI から相手側装置を特定する (ステップ S108c)。インタフェースが専用線であった場合は、直ちに次の処理に進む。

【0042】その後、特定した装置の IP アドレスを自装置の持つ ARP テーブル等から調べ、これを追跡結果として自装置の追跡順序情報と共に管理システム 20 に通知する (ステップ S109)。特定した装置に自装置のものと同様のデータ追跡機構が存在する場合は、この装置宛てに、上記特徴情報と自装置の追跡順序情報とを含む追跡指示を出す (ステップ S110 : Yes、S111)。

【0043】この動作を、特定した装置にデータ追跡機構が存在しなくなるまで繰り返す (ステップ S110 : No)。データ追跡機構が存在しなくなった場合は、自装置が最終のデータ中継装置である旨を含む解析結果と一つ前の装置について特定した IP アドレスとを管理システム 20 に通知して処理を終える。これにより、管理システム 20 では、追跡対象ケットの発信源装置ないしその近傍のシステムを特定することが可能となる。なお、ケットの監視の際、一定の時間を過ぎても該当するケットを捕捉できなかった場合は、該当ケットがもはや流通しないと考えられるので、処理を終える (ステップ S107 : Yes)。この場合は、前述のように、エラーと共に最終である旨を添付して管理システム 20 に通知する。

【0044】管理システム 20 は、各データ中継装置 10 からの通知情報をもとに、追跡対象データの流通経路を特定する。また、最終のデータ中継装置 10 (最終である旨を通知したデータ中継装置 10) からの通知情報をもとに前述の WHOIS データベースその他の外部データベース等を利用して発信源装置を管理するシステムの組織を特定し、必要に応じて警告メールを送出する。

【0045】このように、本実施形態のデータ追跡システム 1 では、送信元の IP アドレスが偽われた場合であっても、その下位層のフレーム等の識別子を解析することにより発信源装置を正しく特定することができる。また、追跡対象データが通ってきた流通経路を特定することもできる。これにより、送信元の IP アドレスを偽ることによる不正者の利益がなくなるため、不正アクセスの抑止効果にもつながる。

【0046】なお、本実施形態では、インターネット上を流通する電子データの発信源を特定する場合の例について説明したが、本発明は、他の通信形態にも応用が可能なものである。また、ケット通信のみならず、画像データその他のコンテンツの流通監視にも応用が可能で

ある。

【0047】

【発明の効果】以上の説明から明らかなように、本発明によれば、電子データを受信した側で、その電子データの送信元を正しく特定できるようになる。

【図面の簡単な説明】

【図1】本発明を適用したデータ追跡システムの構成図。

【図2】本実施形態によるデータ中継装置の機能ブロック構成図。

【図3】(a)は追跡対象となる電子データの構造図、(b)はデータ発信源追跡の原理説明図。

【図4】本実施形態による管理システムの機能ブロック構成図。

【図5】攻撃パターンデータベースの内容の一例を示した図表。

【図6】不正アクセス発信元統計ファイルの内容例を示した図表。

【図7】不正アクセス状況統計ファイルの内容例を示した図表。

【図8】登録センサ情報ファイルの内容例を示した図

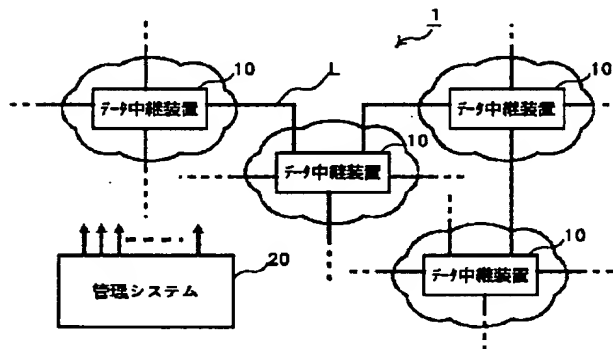
表。

【図9】本実施形態によるデータ追跡システムの運用手順図。

【符号の説明】

- 1 データ追跡システム
- 10 データ中継装置
- 11 指示データ受領部
- 12 データ捕捉部
- 13 データ比較部
- 14 装置等特定部
- 15 通知部
- 20 管理システム
- 21 通信制御機構
- 22 攻撃パターンデータベース
- 23 不正アクセス発信元統計ファイル
- 24 不正アクセス状況統計ファイル
- 25 登録センサ情報ファイル
- 26 追跡指示部
- 27 経路管理部
- 28 警告部
- 30 発信源装置

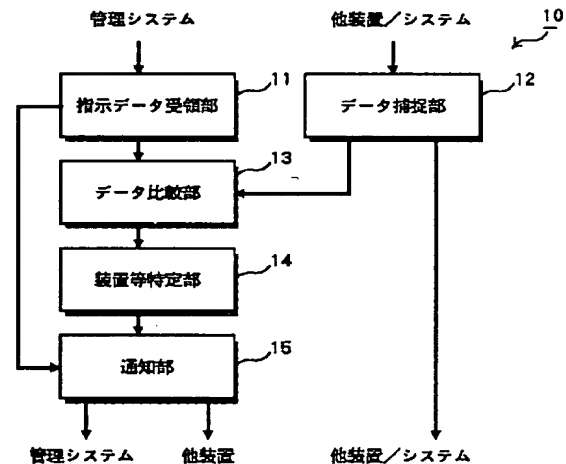
【図1】



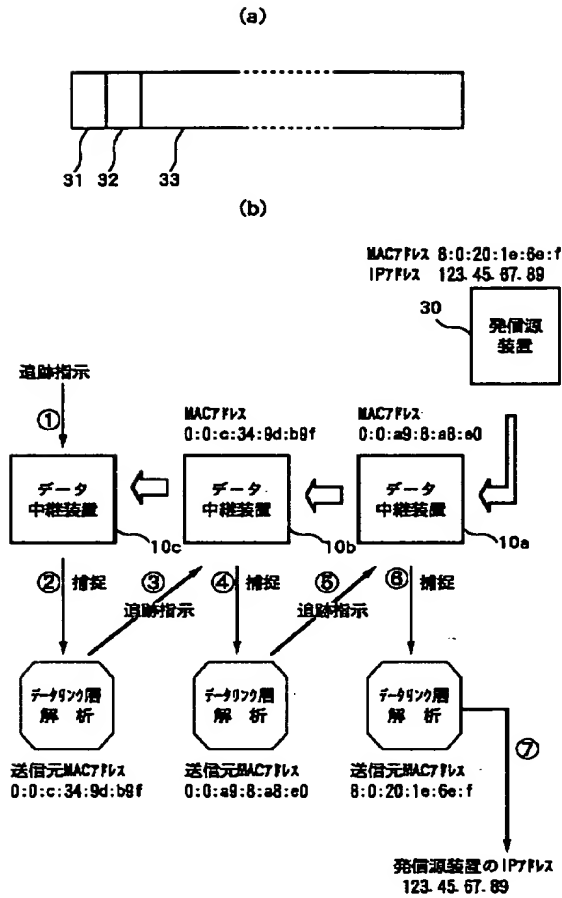
【図5】

攻撃 パターン	S社 センサ	T社 センサ	U社 センサ	...	重要度
A1	P1	Q5	—	...	中
A2	P2	—	—	...	小
A3	P3	Q2	R1	...	大
B1	P4	Q3	R2	...	大
⋮	⋮	⋮	⋮	⋮	⋮

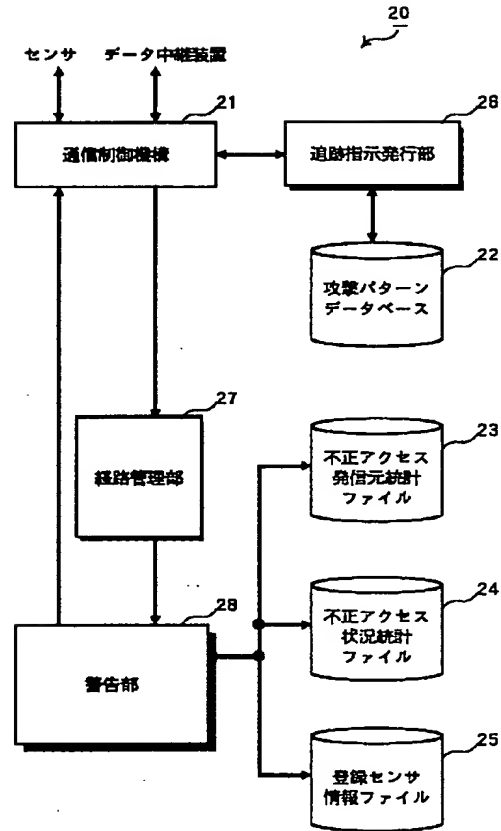
【図2】



【図 3】



【図 4】



【図 7】

【図 6】

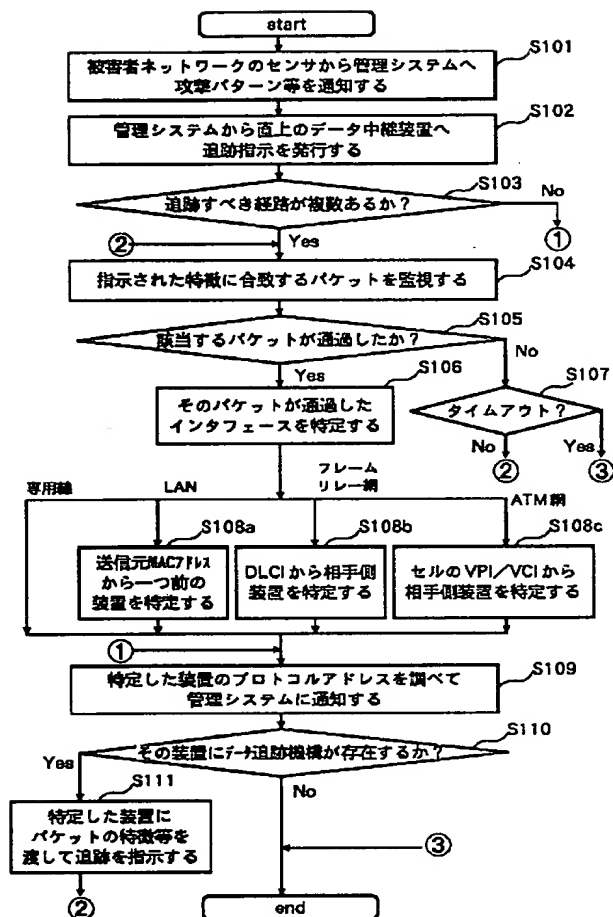
発信元	攻撃パターン	攻撃日時
a1 (10回)	A1 (2回)	1998.10.14
	A2 (5回)	1998.10.16
	B3 (3回)	1998.10.18
a2 (6回)	A2 (3回)	1998.10.20
⋮	⋮	⋮

攻撃パターン	検知数	特記事項
A3	35	
A1	31	
B1	10	
⋮	⋮	⋮

【図 8】

使用センサ 種 別	使用センサ 識別子	管理	直上データ中継 装置07Fb1
S社センサ	S100101	postmaster@a.co.jp	□□□□□
T社センサ	T100201	postmaster@b.co.jp	◇◇◇◇◇
U社センサ	U100301	postmaster@c.co.jp	◎◎◎◎◎
⋮	⋮	⋮	⋮

【図 9】



フロントページの続き

(51) Int. Cl. ⁷

識別記号

F I

テーマコード (参考)

12/66

101 B

12/54

12/58

(72) 発明者 沢沢 博孝

東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内

Fターム(参考) 5B089 GA00 HB02 HB19 JA40 JB16

KA17 KB06 KG05 KG08

5K030 GA11 HA06 HA08 HB14 HC01

HC14 JA11 LB05

5K033 CB08 DA14 DB18 EC03